Researchers tentatively link Greenbug cyberspy group to Saudi Shamoon attackers

scmagazine.com/home/security-news/apts-cyberespionage/researchers-tentatively-link-greenbug-cyberspy-group-to-saudi-shamoon-attackers/

Bradley Barth January 24, 2017

Researchers may have found a tenuous link between a cyberspy organization's credentials-stealing trojan and the Shamoon hacking group that's been targeting Saudi energy companies with Disttrack disk-wiping malware.

According to Symantec, the Greenbug cyberespionage group, known for targeting entities in the Middle East, used the remote access trojan "Ismdoor" to steal credentials from at least one admin computer inside a Saudi organization that was later struck by Disttrack in a wave of attacks on Nov. 17, 2016.

Shamoon's attacks, including one that destroyed 35,000 computers at Saudi oil company Aramco in 2012, require an attacker to use stolen credentials to access the intended victim's systems and implant the Disttrack malware, the company explained in a Monday blog post.

Ismdoor is believed to be exclusively used by Greenbug. The cyberespionage group has been active since at least June 2016 and has targeted organizations across a variety of sectors – including energy – in Saudi Arabia, Iran, Bahrain, Iraq, Qatar, Kuwait and Turkey, the blog post continued.

Symantec believes Greenbug infects its victims via an email that asks recipients to download an RAR file (the format for the WinRAR archiver) that supposedly features a business proposal. In reality, it contains a CHM (Compiled HTML Help) file that includes a Windows alternative data stream, which hides the Ismdoor payload.

Upon execution, Ismdoor opens a backdoor on the infected computer, and leverages Windows PowerShell to set up a command-and-control link used for downloading spy tools that steal credentials and log keystrokes, among other functions.

“The presence of Greenbug within an organization prior to the destructive attack involving W32.Disttrack.B provides only a tentative connection to Shamoon,” the Symantec blog post explains. “Greenbug’s choice of targets and the fact that Ismdoor and associated tools downloaded by the threat appear to have gone quiet a day prior to the November 17, 2016 Shamoon attack is, however, suspicious. At this time, Symantec tracks these groups separately unless additional corroborating evidence emerges.”